CESNET, an association of Czech universities and the Academy of Sciences, represents the Czech Republic in GÉANT. Since the end of last year, CESNET has presented itself under a new logo and the visual style based on it.

Binary code – a kind of DNA of computer science – was the chief inspiration behind the new logotype. Together with the new logo, CESNET started to use a new typeface – Avenir, which is French for ‘future’.

“Undoubtedly, CESNET is an organisation that helps form the future. We provide our services to academic, scientific and research communities as well as other experts. This allows them to get ahead in their fields. That’s why we have chosen Avenir, Future, as our new typeface. We think it’s highly symbolic,” says Gabriela Krčmařová, Head of Communication at CESNET.

The new logo consists of the Association’s name and seven blue squares, which are a graphic representation of the letter ‘c’ in binary-coded ASCII. The authors Petr and Michal Stupka of Radical Design carried out conversion utilising the principle of a Cartesian plane coordinate system with x- and y-axes. If both axes have the same unit of length, we get a square grid in which we can move – a one will always be one row higher than a zero. The transcription of the letter ‘c’ produced a ‘binary smiley’, which has become the Association’s basic graphic symbol.

To spread this word, the conferences sessions focussed on the General Data Protection Regulation (GDPR) that takes effect on May 25 this year and about security threats in daily life. In presence of the National Authority for Data Protection (CNPD-Luxembourg), participants were informed about this new regulation and its compliance control processes in general. Since research projects are concerned by GDPR too, a dedicated session was given about the changes in data protection for future research projects, providing advise and how to adapt to this new regulation.

Besides these GDPR sessions, another one focussed on the need for protecting data. For this, the audience was shown daily threats in information security for raising awareness next to the users to care for their data by illustrating the facility of acquiring data on most different ways. One major factor in the given examples was the human being. Social engineering attacks for stealing valuable information are observed on a daily basis in organization, ranging from phishing to dedicated attacks. Besides these attack, data can also be leaked involuntarily due to badly configured devices, may this be a wrongly configured printer communicating outside of its network or badly configured antennas, routers...

More information and the streamed sessions are available on the University of Luxembourg Twitter account: https://twitter.com/i/moments/957956658134683648.

This was the first conference organized by the University of Luxembourg and the RESTENA Foundation in the framework of the Data Privacy Day and another one will follow next year, so stay tuned!